

the application 30 days past its demise. Following applicant's Petition to Revive, applicant also submits herewith a **Petition for an Extension of Time of 4 Months to File a Response**, 37CFR1.136, to the above designated Office Action. Applicant encloses herewith the required Petition for Revival Fee of **\$750** along with the 4 month Extension Fee of **\$795** totalling **\$1,545**.

5 The unintended delay in responding to the above designated Office Action was incurred due to the file being temporarily misplaced and lost for a period of approximately 3 months incurred during the transfer of the several related files from applicant's prior patent law firm of Knobe, Martens, et al. of Newport Beach, CA to applicant's new patent law firm of English & Associates of Ventura, CA.

In consideration of the granting of the foregoing petitions, applicant submits herewith his **Amendment** and

10 **Response** to the above designated Office Action.

Amendment

37CFR1.121

Please amend the application on file as follows.

In the Claims:

15 Cancel claims 1 - 20, and insert the same information under a new heading, "Objects of the Invention" between "Brief Description of the Invention" and the end of the last paragraph of "Summary of the Invention" on page 11.

Add new claims 21 and 22 as follows:

Claim 21.

20 A secure identification process for networked environments, comprising the steps of:

- capture a photograph of a requester;
- capture a thumbprint of said requester;
- capture a cursive signature of said requester;
- request multiple signatures from a certificate authority (CA) via on line process;
- receive said multiple signatures from said CA via said on line process;
- request a pass phrase from a user;

- encrypt said photograph, thumbprint, cursive signature, and each CA with multiple pass phrases as a key;
- record data on a media multiple times;
- provide user with said media;

5

- prepare a document for signing;
- request said user to insert said media in a compact disc (CD) and digital versatile disc (DVD) drive;
- request said pass phrase from said user;
- use said pass phrase to decrypt said recorded data;

10

- if decryption is not valid, return to "request pass phrase from user step" above;
- if decryption is valid, access said recorded data for signature;
- wrap said prepared document with said received signature;
- attach a public key to said prepared document;
- verify identity of a processor; and

15

- send said prepared document to said processor.

Claim 22.

A secure identification process for networked environments, comprising the steps of:

- capture data from a requester;
- request and generate a pass phrase;
- attach multiple rollover dates to said pass phrase;
- request multiple signatures from a certificate authority (CA) via an online process;
- receive said multiple signatures from said CA via said online process;
- combine said signatures with user data;
- encrypt each said signature and user data with a different combined pass phrase;
- record said user data on media multiple times;
- print a label for front of media;
- provide said user with said media;